Equation $x^i y^j x^k = u^i v^j u^k$ in words

Jana Hadravová and Štěpán Holub

Faculty of Mathematics and Physics, Charles University
186 75 Praha 8, Sokolovská 83, Czech Republic
hadravova@ff.cuni.cz, holub@karlin.mff.cuni.cz

Abstract. We will prove that the word $a^i b^j a^k$ is periodicity forcing if $j \geq 3$ and $i + k \geq 3$, where i and k are positive integers. Also we will give examples showing that both bounds are optimal.

1 Introduction

Periodicity forcing words are words $w \in A^*$ such that the equality $g(w) = h(w)$ is satisfied only if $g = h$ or both morphisms $g, h : A^* \to \Sigma^*$ are periodic. The first analysis of short binary periodicity forcing words was published by J. Karhumäki and K. Culik II in [2]. Besides proving that the shortest periodicity forcing words are of the length five, their work also covers the research of the non-periodic homomorphisms agreeing on the given small word w over a binary alphabet. What in their work attracts attention the most, is the fact, that even short word equations can be quite difficult to solve. The intricacies of the equation $x^2y^3x^2 = u^2v^3u^2$, proved to have only periodic solution [3], nothing but reinforced the perception of difficulty. Not frightened, we will extend the result and prove that the word $a^i b^j a^k$ is periodicity forcing if $j \geq 3$ and $i + k \geq 3$, where i and k are positive integers. Also we will give examples showing that both bounds are optimal.

2 Preliminaries

Standard notation of combinatoric on words will be used: $u \leq_{\mathrm{p}} v$ ($u \leq_{\mathrm{s}} v$ resp.) means that *u is a prefix of v* (*u is a suffix of v* resp.). The maximal common prefix (suffix resp.) of two word $u, v \in A^*$ will be denoted by $u \wedge v$ ($u \wedge_s v$ resp.). By the *length of a word* u we mean the number of its letters and we denote it by $|u|$. A (one-way) *infinite word* composed of infinite number of copies of a word u will be denoted by u^ω. It should be also mentioned that the *primitive root* of a word u, denoted by p_u, is the shortest word r such that $u = r^k$ for some positive k. A word u is *primitive* if it equals to its primitive root. Words u, v are *conjugate* if there are words α, β such that $u = \alpha\beta$ and $v = \beta\alpha$. For further reading, please consult [6].

We will briefly recall a few basic and a few more advanced concepts which will be needed in the proof of our main theorem. Key role in the proof will be played by the Periodicity lemma [6]:

Lemma 1 (Periodicity lemma). *Let p and q be primitive words. If p^ω and q^ω have a common factor of length at least $|p|+|q|-1$, then p and q are conjugate. If, moreover, p and q are prefix (or suffix) comparable, then $p=q$.*

Reader should also recall that if two word satisfy an arbitrary non-trivial relation, then they have the same primitive root. Another well-known result is the fact that the maximal common prefix (suffix resp.) of any two different words from a binary code is bounded (see [6, Lemma 3.1]). We formulate it as the following lemma:

Lemma 2. *Let $X=\{x,y\}$ and let $\alpha \in xX^*$, $\beta \in yX^*$ be words such that $\alpha \wedge \beta \geq |x|+|y|$. Then x and y commute.*

The previous lemma can be formulated also for the maximal common suffix:

Lemma 3. *Let $X=\{x,y\}$ and let $\alpha \in X^*x$, $\beta \in X^*y$ be words such that $\alpha \wedge_s \beta \geq |x|+|y|$. Then x and y commute.*

The most direct and most well known case is the following.

Lemma 4. *Let $s=s_1s_2$ and let $s_1 \leq_{\mathrm{s}} s$ and $s_2 \leq_{\mathrm{p}} s$. Then s_1 and s_2 commute.*

Proof. Directly, we obtain $s=s_1s_2=s_2s_1$.

Next, let us remind the following property of conjugate words:

Lemma 5. *Let $u,v,z \in A^*$ be words such that $uz=zv$. Then u and v are conjugate and there are words $\sigma,\tau \in A^*$ such that $\sigma\tau$ is primitive and*

$$u \in (\sigma\tau)^*, \qquad z \in (\sigma\tau)^*\sigma, \qquad v \in (\tau\sigma)^*.$$

We will also need not so well-know, but interesting, result by A. Lentin and M.-P. Schützenberger [4].

Lemma 6. *Suppose that $x,y \in A^*$ do not commute. Then $xy^+ \cup x^+y$ contains at most one imprimitive word.*

We now introduce some more terminology. Suppose that x and y do not commute and let $X=\{x,y\}$, i.e. we suppose that X is a binary code. We say that a word $u \in X^*$ is *X-primitive* if $u=v^i$ with $v \in X^*$ implies $u=v$. Similarly, $u,v \in X^*$ are *X-conjugate*, if $u=\alpha\beta$ and $v=\beta\alpha$ and the words α and β are from X^*.

In the following lemma, first proved by J.-C. Spehner [7], and consequently by E. Barbin-Le Rest and M. Le Rest [1], we will see that all words that are imprimitive but X-primitive are X-conjugate of a word from the set $x^*y \cup xy^*$.

Source of the inspiration of both articles was an article by A. Lentin and M.-P. Schützenberger [4] with its weaker version stating that if the set of X-primitive words contains some imprimitive words, then so does the set $x^*y \cup xy^*$. As a curiosity, we mention that Lentin and Schützenberger formulated the theorem for $x^*y \cap y^*x$ instead of $x^*y \cup y^*x$ (for which they proved it). Also, the Le Rests did not include in the formulation of the theorem the trivial possibility that the word x or the word y is imprimitive.

Lemma 7. *Suppose that $x, y \in A^*$ do not commute and let $X = \{x, y\}$. If $w \in X^*$ is a word that is X-primitive and imprimitive, then w is X-conjugate of a word from the set $x^*y \cup y^*x$. Moreover, if $w \notin \{x, y\}$, then primitive roots of x and y are not conjugate.*

Putting together Lemma 6 with Lemma 7, we get the following result:

Lemma 8. *Suppose that $x, y \in A^*$ do not commute and let $X = \{x, y\}$. Let $\mathcal{C}$ be the set of all X-primitive words from $X^+ \setminus X$ that are not primitive. Then either $\mathcal{C}$ is empty or there is $k \geq 1$ such that*

$$\mathcal{C} = \{x^i y x^{k-i}, 0 \leq i \leq k\} \text{ or } \mathcal{C} = \{y^i x y^{k-i}, 0 \leq i \leq k\}.$$

The previous lemma finds its interesting application when solving word equations. For example, we can see that an equation $x^i y^j x^k = z^\ell$, with $\ell \geq 2$, $j \geq 2$ and $i + k \geq 2$ has only periodic solutions. (This is a slight modification of a well known result of Lyndon and Schützenberger [5]). Notice, that we can use the previous lemma also with equations which would generate notable difficulties if solved "by hand". E.g. equation

$$(yx)^i yx(xxy)^j xy(xy)^k = z^m,$$

with $m \geq 2$, has only periodic solutions.

We formulate it as a special lemma:

Lemma 9. *Suppose that $x, y \in A^*$ do not commute and let $X = \{x, y\}$. If there is an X-primitive word $\alpha \in X^*$ and a word $z \in A^*$, such that*

$$\alpha = z^i,$$

with $i \geq 2$, then $\alpha = x^k y x^\ell$ or $\alpha = y^k x y^\ell$, for some $k, \ell \geq 0$.

We finish this preliminary part with the following useful lemmas:

Lemma 10. *Let $u, v, z \in A^*$ be words such that $z \leq_{\mathrm{s}} v$ and $uv \leq_{\mathrm{p}} zv^i$, for some $i \geq 1$. Then $uv \in zp_v^*$.*

Proof. Let $0 \leq j < i$ be the largest exponent such that $zv^j \leq_{\mathrm{p}} uv$ and let $r = (zv^j)^{-1}uv$. Then r is a prefix of v. Our assumption that $z \leq_{\mathrm{s}} v$ yields that $v \leq_{\mathrm{s}} vr$ and

$$r(r^{-1}v) = v = (r^{-1}v)r.$$

From the commutativity of words $r^{-1}v$ and r, it follows that they have the same primitive root, namely p_v. Since $uv = (zv^j)r$ we have $uv \in zp_v^*$, which concludes the proof.

Lemma 10 has the following direct corollary.

Lemma 11. *Let $w, v, t \in A^*$ be words such that $|t| \leq |w|$ and $wv \leq_{\mathrm{p}} tv^i$, for some $i \geq 1$. Then $w \in tp_v^*$.*

Proof. Lemma 10 with $u = t^{-1}w$ and z empty yields that $uv \in p_v^*$. Then $wv \in tp_v^*$ and from $|t| \leq |w|$, we obtain that $w \in tp_v^*$.

Lemma 12. *Let $u, v \in A^*$ be words such that $|u| \geq |v|$. If αu is a prefix of v^i and $u\beta$ is a suffix of v^i, for some $i \geq 1$, then $\alpha u \beta$ and v commute.*

Proof. Since $\alpha u \leq_{\mathrm{p}} v^i$ and $|u| \geq |v|$ we have

$$\alpha^{-1} v \alpha \leq_{\mathrm{p}} u \leq_{\mathrm{p}} u\beta.$$

Our assumption that $u\beta$ is a suffix of v^i yields that $u\beta$ has a period $|v|$. Then, $u\beta \leq_{\mathrm{p}} (\alpha^{-1} v \alpha)^i$ and, consequently, $\alpha u \beta \leq_{\mathrm{p}} v^i$. From $v \leq_{\mathrm{s}} u\beta$ and Lemma 10, it follows that $\alpha u \beta \in p_v^*$, which concludes the proof.

Lemma 13. *Let $u, v \in A^*$ be words such that $|u| \geq |v|$. If αu and βu are prefixes of v^i, for some $i \geq 1$, and $|\alpha| \leq |\beta|$, then α is a suffix of β, and $\beta\alpha^{-1}$ commutes with v.*

Proof. Since αu is a prefix of v^+ and $|u| \geq |v|$, we have $\alpha^{-1} v \alpha \leq_{\mathrm{p}} u$. Similarly, $\beta^{-1} v \beta \leq_{\mathrm{p}} u$. Therefore,

$$\alpha^{-1} v \alpha = \beta^{-1} v \beta,$$

and $|\alpha| \leq |\beta|$ yields $\alpha \leq_{\mathrm{s}} \beta$. From $\beta\alpha^{-1} v = v \beta \alpha^{-1}$ we obtain commutativity of v and $\beta\alpha^{-1}$.

Notice that the previous result can be reformulated for suffixes of v^i:

Lemma 14. *Let $u, v \in A^*$ be words such that $|u| \geq |v|$. If $u\alpha$ and $u\beta$ are suffixes of v^i, for some $i \geq 1$, and $|\alpha| \leq |\beta|$, then α is a prefix of β, and $\alpha^{-1}\beta$ commutes with v.*

3 Solutions of $x^i y^j x^k = u^i v^j u^k$

Theorem 1. *Let $x, y, u, v \in A^*$ be words such that $x \neq u$ and*

$$x^i y^j x^k = u^i v^j u^k, \tag{1}$$

where $i + k \geq 3$, $ik \neq 0$ and $j \geq 3$. Then all words x, y, u and v commute.

Proof. First notice that, by Lemma 9, theorem holds in case that either of the words x, y, u or v is empty. In what follows, we suppose that x, y, u and v are non-empty. By symmetry, we also suppose, without loss of generality, that $|x| > |u|$ and $i \geq k$; in particular, $i \geq 2$. Recall that p_x (p_y, p_u, p_v resp.) denote the primitive root of x (y, u, v resp.).

We first prove the theorem for some special cases.

(A) Let $p_x = p_u$.

Then $p_x^{in} y^j p_x^{kn} = v^j$ for some $n \geq 1$, and we are done by Lemma 9.

Notice that the solution of case (A) allows us to assume the useful inequality

$$(i + k - 1)|u| < |p_x|, \tag{$*$}$$

since otherwise p_x^ω and u^ω have a common factor of the length at least $|p_x| + |u|$, and u and x commute by the Periodicity lemma. From

$$(u^{-i+1} p_x u^{-k})u = u(u^{-i} p_x u^{-k+1})$$

and Lemma 5 we see that there are words σ and τ such that $\sigma\tau$ is primitive and

$$(u^{-i+1} p_x u^{-k}) \in (\sigma\tau)^m, \qquad u = (\sigma\tau)^\ell \sigma, \qquad u^{-i+1} p_x u^{-k} \in (\tau\sigma)^m,$$

for some $m \geq 1$ and $\ell \geq 0$. Then we have

$$u = (\sigma\tau)^\ell \sigma, \qquad p_x = u^i (\tau\sigma)^m u^{k-1} = u^{i-1} (\sigma\tau)^m u^k, \tag{$**$}$$

for some $m \geq 1$ and $\ell \geq 0$.

(B) Let p_y and p_v be conjugate.

Let α and β be such that $p_y = \alpha\beta$ and $p_v = \beta\alpha$. Since $x^i p_y$ is a prefix of $u^i p_v^+$, we can see that $u^{-i} x^i \alpha\beta \leq_{\mathrm{p}} \beta(\alpha\beta)^+$. From Lemma 10 we infer that and $u^{-i} x^i \in \beta(\alpha\beta)^*$. Similarly, by the mirror symmetry, $p_y x^k \leq_{\mathrm{s}} p_v^+ u^k$ yields that $x^k u^{-k} \in (\alpha\beta)^* \alpha$. Then

$$x^{i+k} = u^i p_v^n u^k,$$

for some $n \geq 1$. From $|v| > |y|$, it follows that $|v| \geq |y| + |p_v|$ and, consequently,

$$(i + k)(|x| - |u|) = j(|v| - |y|) \geq 3|p_v|.$$

Then $n \geq 3$ and we are done by Lemma 9.

(C) Let p_x and p_v be conjugate.

Let α and β be such that $p_x = \alpha\beta$ and $p_v = \beta\alpha$. From $(*)$ and $i \geq 2$, it follows that $u^i p_v$ is a prefix of p_x^2. Then $u^i(\beta\alpha) \leq_{\mathrm{p}} \alpha(\beta\alpha)^+$ and Lemma 10 yields that $u^i \in \alpha(\beta\alpha)^*$. From $i|u| < |p_x|$, it follows $u^i = \alpha$. Since p_x is a suffix of $\alpha\beta\alpha u^k = p_x u^{i+k}$ and u is a prefix of p_x, we deduce from Lemma 3 that x and u commute, case (A).

We will now discuss separately cases when $|x| \geq |v|$ and $|x| < |v|$.

1. Suppose that $|x| \geq |v|$.

If $i \geq 3$ or $x \neq p_x$, then $(u^{-i}x)x^{i-1}$ is a prefix of v^j that is longer than $|p_x| + |x|$ by $(*)$. By the Periodicity lemma, p_x is a conjugate of p_v and we are in case (C). The remaining cases deal with $i = k = 2$ and $i = 2$, $k = 1$.

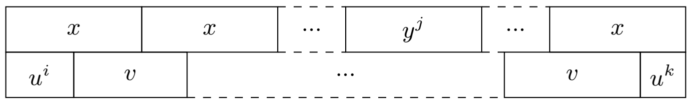

Figure 1. Case $|x| \geq |v|$.

1a) First suppose that $i = k = 2$. Since $(u^{-i}x)x$ is a prefix of v^j and $x(xu^{-k})$ is a suffix of v^j, we get, by Lemma 12, that $(u^{-i}x)x(xu^{-k})$ commutes with v. Then

$$x^3 = u^i p_v^n u^k,$$

for some $n \geq 0$. From $(i + k - 1)|u| < |p_x| \leq |x|$ and $|p_v| \leq |v| \leq |x|$ we infer that $n \geq 2$. Therefore, $p_u = p_x$ holds by Lemma 9, and we have case (A).
1b) Suppose now that $i = 2$ and $k = 1$. We will have a look at the words u and $x = p_x$ expressed by $(**)$. Let $h = (\sigma\tau)^m$ and $h' = (\tau\sigma)^m$. Then $(**)$ yields

$$u = (\sigma\tau)^\ell\sigma, \qquad\qquad x = u^2h' = uhu.$$

1b.i) Suppose now that $|p_v| \leq |uh|$. Since $h'uh$ is a prefix of v^j and uh is a suffix of v^j, we obtain by Lemma 12 that $h'uh = p_v^n$. From $|p_v| \leq |uh|$, we infer $n \geq 2$ and, according to Lemma 9, σ and τ commute. Then also x and u commute and we have case (A).
1b.ii) Suppose that $|p_v| > |uh|$. From $|x| \geq |v| \geq |p_v|$, it follows that $p_v = h'uu_1$ for some prefix u_1 of u. We can suppose that u_1 is a proper prefix of u, otherwise x and v are conjugate and we have case (C). Then $u_1h' \leq_{\mathrm{p}} uh' \leq_{\mathrm{p}} (\sigma\tau)^+$ and, by Lemma 13, we obtain $uu_1^{-1} \in (\sigma\tau)^+$. Therefore, $u_1 \in (\sigma\tau)^*\sigma$. Since $h \leq_{\mathrm{s}} p_v$, we can see that $\sigma\tau \leq_{\mathrm{s}} \tau\sigma^+$. Lemma 3 then implies commutativity of σ and τ. Therefore, the words x and u also commute and we are in case (A).

2. Suppose that $|x| < |v|$ and $i|x| = i|u| + |v|$.
From $x \leq_{\mathrm{s}} v$, we have $x \leq_{\mathrm{s}} xu^k$. Since $u \leq_{\mathrm{p}} x$ we deduce from Lemma 3 that x and u commute, thus we have case (A).

3. Suppose that $|x| < |v|$ and $i|x| > i|u| + |v|$.

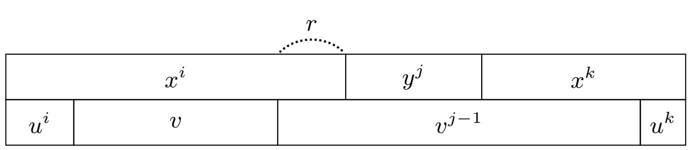

Figure 2. Case $|x| < |v|$ and $i|x| > i|u| + |v|$.

Let r be a non-empty word such that $u^ivr = x^i$. Notice that $|r| < |p_x|$ otherwise the words p_x and p_v are conjugate and we have case (C). Considering

the words u and p_x expressed by $(**)$, we can see that $(\tau\sigma)^m u^{k-1}u^i$ is a prefix of v and $u^{i-1}(\sigma\tau)^m$ is a suffix of v. Notice also that we have case (A) if σ and τ commute.

3a) Consider first the special case when $r = u^k$.

3a.i) If $i = k$, then $v^{j-2} = u^i y^j u^i$. If $j \geq 4$, we have case (B) by Lemma 9. If $j = 3$, then the equality $u^i v r = x^i$ implies $x^i = u^{2i} y^j u^{2i}$ and we get case (A) again by Lemma 9.

3a.ii) Suppose therefore that $k < i$. Notice that $u = \sigma$, otherwise, from $\tau\sigma \leq_{\mathrm{p}} v$ and $u^k = r \leq_{\mathrm{p}} v$, we get commutativity of σ and τ. Therefore,

$$v \in (\tau\sigma)^m \sigma^{k-1} p_x^* \sigma^{i-1} (\sigma\tau)^m.$$

We have

$$vu^k x^{-k} = vrx^{-k} = u^{-i} x^{i-k}.$$

From $i > k$ and $(*)$ we get $|u^{-i}x^{i-k}| > 0$ and, consequently, $|vu^k| > |x^k|$. Let v' dente the word $vu^k x^{-k}$. Then $v^{j-2}v' = ry^j$, and $j \geq 3$ together with $|v| > |x| > |u^k| = |r|$ yields that v' is a suffix of y^j. According to $(**)$, $v' = u^{-i}x^{i-k} \in (\tau\sigma)^m \sigma^{k-1} p_x^*$. Then, σ^k is a suffix of y^j and we have

$$(\sigma^k y \sigma^{-k})^j = \sigma^k y^j \sigma^{-k} = v^{j-2} v' \sigma^{-k}.$$

This is a point where Lemma 9 turns out to be extremely useful. Direct inspection yields that $v^{j-2}v'\sigma^{-k}$ is not a jth power of a word from $\{\sigma, \tau\}^*$. One can verify, for example, that the expression of $v^{j-2}v'\sigma^{-k}$ in terms of σ and τ contains exactly $j-2$ occurrences of τ^2. Therefore, Lemma 9 yields that σ and τ commute, a contradiction.

3b) We first show that $r = u^k$ holds if $k \geq 2$. Indeed, if $k \geq 2$ then $u^k p_x u^{-k}$ is a suffix of v and, consequently, $u^k p_x u^{-k} r$ is a suffix of x^i. Since $u^k p_x u^{-k} u^k$ is also a suffix of x^i, we can use Lemma 14 and get commutativity of x with one of the words $u^{-k}r$ or $r^{-1}u^k$. From $|r| < |p_x|$ and $|u^k| < |p_x|$, we get $r = u^k$.

3c) Suppose that $k = 1$ and $r \neq u$.

3c.i) If $|r| < |u|$, then r is a suffix of u and $|xr^{-1}u| > |x|$. Since $xr^{-1} \leq_{\mathrm{s}} v$ and $k = 1$, the word $x = xr^{-1}r$ is a suffix of $xr^{-1}u$. Therefore, xr^{-1} is a suffix of $(ur^{-1})^+$. Since $u^2 \leq_{\mathrm{p}} x$ and $|xr^{-1}| \geq |u| + (|u| - |r|)$, the Periodicity lemma implies that the primitive root of ur^{-1} is a conjugate of p_u. But since p_u is prefix comparable with ur^{-1}, we obtain that $ur^{-1} \in p_u^+$. Then also $r \in p_u^+$ and $xr^{-1} \in p_u^+$. Consequently, x and u commute, and we have case (A).

3c.ii) Suppose therefore that $|r| > |u|$. Then u is a suffix of r. Since r is a suffix of p_x and $p_x = u^i(\tau\sigma)^m$, the word r is a suffix of $u^i(\tau\sigma)^m$. From $|v| > |x|$ we obtain $u^{-i}xu^i \leq_{\mathrm{p}} v$. Consequently, from $p_x = u^i(\tau\sigma)^m$ and $r \leq_{\mathrm{p}} v$, it follows that r is a prefix of $(\tau\sigma)^m u^i$.

Consider first the special case when $r \in (\tau\sigma)^m p_u^*$. If $r \in (\tau\sigma)^m p_u^+$, then $r \leq_{\mathrm{s}} u^i(\tau\sigma)^m$ yields that $(\tau\sigma)^m$ and u commute by Lemma 3. Consequently, σ and τ commute, and we have case (A). Therefore, $r = (\tau\sigma)^m$, $p_x = u^i r$ and $v = u^{-i}x^i r^{-1} \in (ru^i)^+$. We have proved that x and v have conjugate primitive roots, which yields case (C). Consider now the general case.

If $m \leq \ell$, then $(\tau\sigma)^m$ is a suffix of u. Since r is a prefix of $(\tau\sigma)^m u^i$, and $u \leq_{\mathrm{s}} r$, we get from Lemma 10 the case $r \in (\tau\sigma)^m p_u^*$.

Suppose that $m > \ell$. Then u is a suffix of $(\tau\sigma)^m$. Let s denote the word $(\tau\sigma)^m u^{-1} = (\tau\sigma)^{m-\ell-1}\tau$.

If $|r| \geq |(\tau\sigma)^m|$, then $r = s'su$ for some s'. From $r \leq_{\mathrm{p}} (\tau\sigma)^m u^i$, it follows that $s'su$ is a prefix of su^{i+1}. Lemma 11 then yields $s's \in sp_u^*$. Therefore $r \in sup_u^*$ and from $su = (\tau\sigma)^m$, we have the case $r \in (\tau\sigma)^m p_u^*$.

Let $|r| < |(\tau\sigma)^m|$. From $|r| > |u|$ and $(\tau\sigma)^m = su$, we obtain that there are words s_1, s_2 such that $s = s_1 s_2$, $r = s_2 u \leq_{\mathrm{p}} v$ and $s_1 \leq_{\mathrm{s}} v$. Since s is both a prefix and a suffix of v, Lemma 4 implies that s_1 and s_2 have the same primitive root, namely p_s.

Note that $p_x = u^i su$. We now have

$$u^i s_2 s_1 = u^i s \leq_{\mathrm{s}} v \leq_{\mathrm{s}} x^i r^{-1} \leq_{\mathrm{s}} (u^i su)^{i-1} u^i s_1.$$

From $i \geq 2$, it follows that $u^i s_2$ is a suffix of $(u^i su)^{i-1} u^i$ for some $n \geq 1$. Lemma 3 then yields commutativity of s and u. Hence, words x and u also commute and we are in case (A).

4. Suppose now that $|x| < |v|$ and $i|x| < i|u| + |v|$.

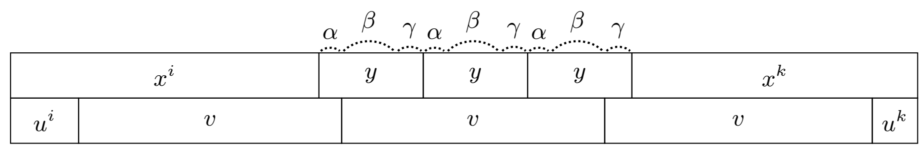

Figure 3. Case $|x| < |v|$ and $i|x| < i|u| + |v|$.

First notice that in this case also $k|x| < k|u| + |v|$. If $j|y| \geq |v| + |p_y|$, then, by the Periodicity lemma, p_v and p_y are conjugate, and theorem holds by (B). Assume that $j|y| < |v| + |p_y|$. Then, since $i|x| < i|u| + |v|$ and $k|x| < k|u| + |v|$, we can see that $j = 3$ and there are non-empty words α, β and γ for which $y = \alpha\beta\gamma$ and $v = (\beta\gamma)(\alpha\beta\gamma)(\alpha\beta)$, with $|\alpha\gamma| < |p_y|$.

4a) Suppose first that $|u^i\gamma| \leq |x|$. Notice that also $|\alpha u^k| \leq |x|$ since $k \leq i$ and $|\gamma| = (i-k)(|x|-|u|)+|\alpha|$. Then $|\gamma x| \leq |v|$ and $u^i\gamma x$ is a prefix of x^2. Therefore, by Lemma 10, $u^i\gamma$ commutes with x. We obtain the following equalities:

$$v = \gamma p_x^n \alpha, \qquad\qquad y^j = \alpha v \gamma = (\alpha\gamma) p_x^n (\alpha\gamma),$$

where $n \geq 1$. If $n \geq 2$, then x and y commute by Lemma 9. If $n = 1$, then $p_x = x$ and $i = 2$. Since $\gamma x^k = vu^k = \gamma x \alpha u^k$ and $|\alpha u^k| \leq |x|$, also $k = 2$ and $\alpha u^k = x$. Then $|\alpha| = |\gamma|$ and $u^2\gamma = x = \alpha u^2$. If $|u| \geq |\gamma|$, then u and γ commute, a contradiction with $p_x = x$. Therefore, $|x| < 3|\gamma|$ and $|v| = |\gamma x \alpha| < 5|\gamma|$. Since γ is a suffix of x and α is a prefix of x, $(\gamma\alpha\beta)^3\gamma\alpha$ is a factor of v^3 longer than $|y| + |v|$. Therefore, by the Periodicity lemma, words y and v are conjugate, and

we have case (B).

4b) Suppose that $|u^i\gamma| > |x|$, denote $z = x^{-1}u^i\gamma$ and $z' = \gamma^{-1}v\alpha^{-1} = x^k u^{-k}\alpha^{-1}$. From

$$|y| + |\gamma| + |\alpha| < |v| = |\gamma z'\alpha|,$$

we deduce $|y| < |z'|$. Since $x^{i-1} = zz'$ and z' is a prefix of x^k, the word zz' has a period $|z| < |\gamma|$. Since zz' is a factor of v greater than $|z| + |y|$ and v has a period $|p_y|$, the Periodicity lemma implies $|p_y| \leq |z| < |\gamma|$, a contradiction with $|\gamma| < |p_y|$. □

4 Conclusion

The minimal bounds for i, j, k in the previous theorem are optimal. In case that $i = k$ and j is even, Eq. (1) splits into two separate equations, which have a solution if and only if either $i = k$ and $j = 2$, or $i = k = 1$, see [2].

Apart from these solutions, we can find non-periodic solutions also in case that $i \neq k$. Namely, for $j = 2$ and $i = k + 1$, we have

$$\begin{aligned} x &= \alpha^{2k+1}(\beta\alpha^k)^2, & u &= \alpha, \\ y &= \beta\alpha^k, & v &= (\alpha^k\beta)^2(\alpha^{3k+1}\beta\alpha^k\beta)^k. \end{aligned}$$

So far this seems to be the only situation when the equation

$$x^i y^2 x^k = u^i v^2 u^k \tag{2}$$

with $i > k$ has a non-periodic solution. We conjecture that if $|i - k| \geq 2$, then Eq. (2) has only periodic solutions.

If $i = k = 1$ and j is odd, then Eq. (1) has several non-periodic solutions, for example:

$$\begin{aligned} x &= \alpha\beta\alpha, & u &= \alpha, \\ y &= \gamma, & v &= \alpha\gamma^j\alpha, \end{aligned}$$

where $\beta^2 = v^{j-1}$.

References

1. Evelyne Barbin-Le Rest and Michel Le Rest. Sur la combinatoire des codes à deux mots. *Theor. Comput. Sci.*, 41:61–80, 1985.
2. Karel Culik II and Juhani Karhumäki. On the equality sets for homomorphisms on free monoids with two generators. *ITA*, 14(4):349–369, 1980.
3. Elena Czeizler, Štěpán Holub, Juhani Karhumäki, and Markku Laine. Intricacies of simple word equations: an example. *Internat. J. Found. Comput. Sci.*, 18(6):1167–1175, 2007.

4. A. Lentin and M.-P. Schützenberger. A combinatorial problem in the theory of free monoids. In G. Pollak, editor, *Algebraic theory of semigroups / edited by G. Pollak*. North-Holland Pub. Co Amsterdam ; New York, 1979.
5. R. C. Lyndon and M.-P. Schützenberger. The equation $a^m = b^n c^p$ in a free group. *The Michigan Mathematical Journal*, 9(4):289–298, 12 1962.
6. Grzegorz Rozenberg and Arto Salomaa, editors. *Handbook of formal languages, vol. 1: word, language, grammar*. Springer-Verlag New York, Inc., USA, 1997.
7. J.-P. Spehner. *Quelques problèmes d'extension, de conjugaison et de presentation des sous-monoïdes d'un monoïde libre*. PhD thesis, Université Paris VII, Paris, 1976.